10/525213 PCT/EP03/08022 14.08.03

BUNDESREPUBLIK DEUTSCHLAND

PCT/EP03/8022

REC'D 28 AUG 2003
WIPO PCT

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 38 095.3

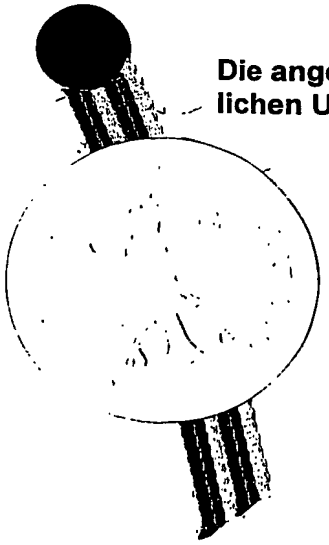
Anmeldetag: 21. August 2002

Anmelder/Inhaber: AUDI AG, Ingolstadt/DE

Bezeichnung: Verfahren zum Schutz vor Manipulation an einem Steuergerät für mindestens eine Kfz-Komponente und Steuergerät

IPC: B 60 R 16/02

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.



München, den 31. Juli 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Sleck

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

A 9161
02/00
EDV-L

BEST AVAILABLE COPY

IP 4537c
Th/Sc

Verfahren zum Schutz vor Manipulationen an einem Steuergerät für mindestens eine Kfz-Komponente und Steuergerät

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zum Schutz vor Manipulationen an einem Steuergerät für mindestens eine Kfz-Komponente und ein Steuergerät, in dem dieses Verfahren realisiert ist.

In Kraftfahrzeugen werden heutzutage zur Steuerung einzelner Kfz-Komponenten Steuergeräte verwendet, wie beispielsweise das Motorsteuergerät oder das Getriebesteuergerät. Die zum Betrieb von solchen Steuergeräten erforderlichen Informationen, wie beispielsweise Programme und Daten, werden verschlüsselt oder unverschlüsselt in Speicherbausteinen (E^2PROM, Flash und dergleichen) abgelegt. Das Verschlüsselungsverfahren ist dabei unabhängig von einer festen Hardware-Kombination von Bausteinen und in der Regel in einem wiederbeschreibbaren Speichermedium abgelegt.

Der Nachteil solcher Steuergeräte und der verwendeten Programme besteht darin, dass einzelne Speicherbausteine ausgetauscht werden können, bzw. die Daten auf den Speicherbausteinen über eine Diagnoseschnittstelle oder über direkten Zugriff auf den Speicherbaustein überschrieben werden können. Der Austausch eines Speicherbausteins oder das Überschreiben der auf diesem Speicherbaustein gespeicherten Daten und Programme kann, dazu führen, dass die Kfz-Komponente mit anderen Kenndaten arbeitet. Dies wird beispielsweise bei dem sogenannten Chip-Tuning durchgeführt, bei dem Speicherbausteine, die dem Motorsteuergerät zugeordnet sind, ausgetauscht bzw. die auf diesen Speicherbausteinen gespeicherten Programme und Daten, wie Kenndaten, geändert werden. Dadurch kann beispielsweise eine Erhöhung der Leistung oder des Drehmoments des Motors erzielt werden. Wird diese Manipulation durchgeführt ohne die weiteren Kfz-Komponenten, wie zum Beispiel Turbolader, Ölkühler oder Bremsen anzupassen, so kann es zu Schäden an diesen Kfz-Komponenten und sicherheitskritischen Zuständen kommen.

Aufgabe der vorliegenden Erfindung ist es daher, ein Verfahren zum Schutz vor Manipulation an einem Steuergerät zu schaffen, bei dem ein Austausch eines Speicherbausteins und die Änderung der Daten auf dem Speicherbaustein nicht möglich ist, ohne die Funktionsfähigkeit des Steuergeräts zu beeinflussen oder zumindest die Veränderung zu diagnostizieren und diese ggf. zur Anzeige zu bringen.

Der Erfindung liegt die Erkenntnis zugrunde, dass diese Aufgabe gelöst werden kann, indem eine Verschlüsselung der Daten, die auf einem Speicherbaustein abgelegt sind, verwendet wird, die ausschließlich von dem dem Speicherbaustein ursprünglich zugeordneten Microrechner entschlüsselt werden kann.

Die Aufgabe wird daher gelöst durch ein Verfahren zum Schutz vor Manipulation eines Steuergeräts für mindestens eine Kfz-Komponente, wobei das Steuergerät zumindest einen Microrechner und mindestens einen Speicherbaustein umfasst, wobei zumindest einer der Speicherbausteine einen reversiblen Festwertspeicher darstellt, dadurch gekennzeichnet, dass, in den reversiblen Festwertspeicher Daten abgelegt werden, die durch ein Verschlüsselungsverfahren verschlüsselt worden sind, und der in dem Verschlüsselungsverfahren verwendete Schlüssel zumindest einen Teil mindestens einer ursprünglichen bausteinspezifischen Kennung mindestens eines der Bausteine des Steuergeräts umfasst.

Durch das Integrieren zumindest eines Teils der spezifischen Kennung mindestens einer der ursprünglich in dem Steuergerät eingesetzen Bausteine des Steuergeräts kann eine sinnvolle Entschlüsselung nur von dem Microrechner aus erfolgen, der ursprünglich dem Speicherbaustein zugeordnet war. Ein Austauschen des reversiblen Speicherbausteins, der beispielsweise ein EEPROM darstellen kann, mit den dazugehörigen Daten ist daher nicht möglich.

Vorzugsweise stellt die Kennung, die in dem Schlüssel zum Entschlüsseln der Daten, die auf dem Festwertspeicher gespeichert sind, verwendet wird, eine Kennung des Microrechners dar. Vorzugsweise ist diese Kennung die Identifikationsnummer, die bei der Herstellung des Microrechners vergeben und in diesem abgelegt wird.

Zusätzlich oder alternativ kann die Kennung aber auch eine Kennung eines weiteren Speicherbausteins des Steuergeräts darstellen. So kann beispielsweise die Identifikationsnummer eines mit dem Microrechner verbundenen oder in diesem integrierten Flash-Speichers als Kennung dienen. Dadurch wird der Austausch einzelner Bauteile des Steuergeräts noch weiter erschwert.

Um das Auslesen des Schlüssels, der zumindest teilweise die ursprünglichen Kennungen zumindest eines Teils der Bausteine des Steuergeräts umfasst, zu vermeiden, kann der Schlüssel in dem RAM des Microrechners abgelegt werden. Diese Ausführungsform ist insbesondere dann zu bevorzugen, wenn bei jeder Inbetriebnahme des Steuergeräts der Schlüssel zum Entschlüsseln der in dem reversiblen Festspeicher verschlüsselt abgelegten Daten neu erzeugt werden soll. Dieses Erzeugen des Schlüssels gewährt eine zusätzliche Sicherheit gegen den Austausch einzelner Komponenten des Steuergeräts.

Vorzugsweise wird zur Erzeugung eines Schlüssels zum Entschlüsseln von Daten auf einem reversiblen Festwertspeicher aus einem lesegeschützten, nur einmalig beschreibbaren (one-time-programmable) OTP-Bereich des Microrechners mindestens ein Teil einer Kennung mindestens eines der Bausteine des Steuergeräts ausgelesen.

Die Erfindung wird im Folgenden anhand der beiliegenden Zeichnungen, die sich auf mögliche Ausführungsbeispiele der Erfindung beziehen, beschrieben. Es zeigen:

Figur 1 und 1a: Flußdiagramme, die den Verlauf des erfindungsgemäßen Verfahrens schematisch wiedergeben;

Figur 2: eine schematische Blockdarstellung einer Ausführungsform eines Steuergeräts zum Ausführen des erfindungsgemäßen Verfahrens; und

Figur 3: eine schematische Blockdarstellung einer weiteren Ausführungsform eines Steuergeräts zum Ausführen des erfindungsgemäßen Verfahrens.

In Figur 1 ist der Ablauf des erfindungsgemäßen Verfahrens schematisch in einem Flußdiagramm angedeutet und wird im folgenden erläutert.

Bei der ersten Inbetriebnahme eines Steuergeräts werden die Daten, die in dem E²PROM, das dem Microrechner zugeordnet ist, oder in diesem integriert ist, abgelegt sind, ausgelesen. Parallel oder zeitlich versetzt werden Kennungen, wie beispielsweise die Identifikationsnummern des Microrechners oder weiterer Speicherbausteine, ausgelesen und aus diesen ein Schlüssel gebildet. Mittels dieses Schlüssels werden dann die aus dem E²PROM ausgelesenen Daten verschlüsselt und in dieser verschlüsselten Form in dem E²PROM wieder abgelegt. Im Anschluß daran werden, sobald der Microcomputer auf die Daten des E²PROMs zugreift, diese Daten durch den ursprünglich gebildeten Schlüssel entschlüsselt. Dadurch kann das Steuergerät mit den in dem E²PROM gespeicherten Daten, beispielsweise Adaptionswerte und Anpassungswerte bei einem Motorsteuergerät, vorschriftsgemäß funktionieren.

Bei einer weiteren Betätigung und jeder danach folgenden Betätigung des Steuergeräts werden erneut zumindest ein Teil der Kennungen zumindest eines Bausteins des Steuergeräts, wie beispielsweise des Microrechners, ausgelesen und ein Schlüssel aus diesen Kennungen oder einem Teil dieser Kennungen erzeugt. Erfolgt im Anschluss daran ein Zugriff auf die in dem E²PROM abgelegten Daten, die mittels des ursprünglichen Schlüssels verschlüsselt wurden, so werden bei Identität der dem Microrechner zugeordneten Speicherbausteine und des E²PROMS die verschlüsselten Daten durch den neu erneut erzeugten Schlüssel entschlüsselt und können in dem Microrechner zur Steuerung der zugeordneten Kfz-Komponente verwendet werden. Wurde hingegen einer der Bausteine ausgetauscht, so stimmt der von dem Microrechner erzeugte Schlüssel zum Entschlüsseln nicht mit der Verschlüsselung überein und auf die auf dem E²PROM abgelegten Daten kann nicht korrekt zugegriffen werden.

Weitere Ausführungsformen des erfindungsgemäßen Verfahrens werden unter Bezugnahme auf die Figuren 2 und 3 beschrieben.

In Figur 2 ist eine Ausführungsform eines Steuergeräts dargestellt. Der Aufbau von Steuergeräten, wie beispielsweise Motorsteuergeräten, ist hinlänglich aus dem Stand der Technik bekannt, so dass hierauf nur insoweit eingegangen wird, wie dies für das Verständnis der Erfindung erforderlich ist. Das Steuergerät 1 umfasst in der dargestellten Ausführungsform einen Microcomputer µC, einen Flash-Speicher 2 und einen EEPROM (E²PROM) 3. Der Flash-Speicher 2 und der E²PROM 3 weisen jeweils einen OTP-Bereich 21,

31 auf. Diese sind vorzugsweise nicht lesegeschützt ausgestaltet. Auch in dem μC ist ein OTP-Bereich 11 vorgesehen.

Die Speicherbausteine Flash 2, E²PROM 3 sind in der dargestellten Ausführungsform mit bausteinindividuellen Identifikationsnummern ID versehen. Diese werden in der Regel beim Hersteller des Bausteins geschrieben und in den OTP-Bereich 21, 31 der einzelnen Bausteine abgelegt.

Im Herstellungsprozess des Steuergeräts werden bei der Erstinbetriebnahme des Steuergeräts von dem Microrechner μC die ID's der einzelnen Speicherbausteine 2, 3 ausgelesen und in einen einmalig beschreibbaren OTP-Bereich 11 des μC abgelegt. Ab diesem Zeitpunkt ist die Funktion des Steuergeräts 1 nur in Verbindung mit den dem μC bekannten ID's der externen Speicherbausteine 2, 3 möglich.

Bei jeder weiteren Inbetriebnahme des Steuergeräts 1 wird von dem μC die ID aller mit diesem verbundenen Speicherbausteine 2, 3 erneut ausgelesen. In einer Vergleichseinheit können dann diese aktuellen ID's mit den ursprünglichen Kennungen, die in dem OTP-Bereich 11 des μC abgelegt sind, verglichen werden. Wird bei diesem Vergleich festgestellt, dass eine der ID's nicht mit einer der ursprünglichen ID's übereinstimmt, so wird das Steuergerät an seiner Funktion gehindert oder zumindest die Veränderung diagnostiziert und diese ggf. zur Anzeige gebracht.

Der Code zum Betreiben des Steuergeräts ist in einen Master-Code (MC) und einen Sub-Code (SC) unterteilt. Der Mastercode MC enthält elementare, essentielle Funktionalitäten zum Betrieb des Steuergeräts, z.B. das Programm zur Signalerzeugung für an das Steuergerät angeschlossene Aktuatoren (nicht dargestellt) oder das Programm für die Berechnung der Stellgrößen und Stellwerte. Der Mastercode MC kann weiterhin Daten umfassen. In dem Sub-Code SC sind weitere Programme und Daten enthalten. Das Steuergerät ist nur funktionsfähig unter Verwendung beider Codes MC und SC. In der dargestellten Ausführungsform ist der Sub-Code SC in einem wiederbeschreibbaren Bereich des Flash-Speichers 2 enthalten. Der Master-Code MC ist in einem OTP-Bereich 11 des Microrechners μC enthalten. Der Master-Code ist vorzugsweise gegen Auslesen über Kontaktierung geschützt. Dies kann beispielsweise physikalisch durch Durchlegieren einer Transistorstrecke oder schaltungstechnisch erzielt werden. Der Sub-Code SC kann im Ge-

gesatz zu dem Master-Code MC modifiziert beziehungsweise überschrieben werden. Dies erlaubt ein Updaten des Subcodes oder ein Reprogrammieren.

Der μC weist weiterhin eine Identifikationsnummer μC-ID auf. Auch diese ist in einem lesegeschützten OTP-Bereich des μC abgelegt. In dem E²PROM sind weitere Daten für den Betrieb des Steuergeräts in einem wiederbeschreibbaren Bereich abgelegt. Diese Daten können beispielsweise Adaptionswerte sowie Leerlaufdrehzahlen sein.

Beim Initialisieren des Steuergeräts lernt der Microrechner μC die in dem OTP-Bereich 21, 31 der Speicherbausteine 2, 3 abgelegten und dadurch nicht veränderbaren Identifikationsnummern an und legt diese in einem OTP-Bereich des Microrechners μC, der optional auch lesegeschützt ausgestaltet sein kann, ab.

Von diesem Zeitpunkt an sind dem Microrechner μC die mit diesem verbundenen Speicherbausteine 2, 3 über ihre ID bekannt.

Zusätzlich können die in dem Microrechner abgelegten ID's der Speicherbausteine auch zur Verschlüsselung von Daten oder Programmen dienen. So können die auf dem E²PROM abgelegten Daten beispielsweise durch ein symmetrisches Verschlüsselungsverfahren codiert werden, in dem der Schlüssel zumindest einen Teil der ID zumindest eines der Speicherbausteine 2, 3 umfasst. Bei einem Motorsteuergerät können in dem E²PROM beispielsweise Kennfelder, wie , Lernwerte, Fertigungsdaten und Anpassungswerte, gespeichert sein. Zur Verschlüsselung sind grundsätzlich alle symmetrischen Verschlüsselungsverfahren geeignet, die die Einbeziehung eines steuergeräteindividuellen Kennzeichnens erlauben. Vorzugsweise werden die Daten des E²PROM durch einen Schlüssel verschlüsselt, der zusätzlich oder alternativ zu der ID der externen Speicherbausteine die ID des Microrechners μC umfasst. Hierdurch wird eine steuergeräteindividuelle Verschlüsselung erzielt, die ein Austauschen des E²PROMs oder ein Überschreiben der darauf gespeicherten Daten unmöglich macht bzw. den Betrieb des Steuergeräts nach einer solchen Manipulation verhindert. Der Schlüssel wird vorzugsweise in dem RAM-Speicher des Microrechners μC abgelegt. Dadurch wird der Schlüssel bei jedem Hochlaufen des Steuergeräts unter Einbeziehung eines steuergeräteindividuellen Kennzeichens (z.B. der ID des μC und gegebenenfalls der ID's der Speicherbausteine) gebildet und ist somit steuergeräteindividuell.

Weiterhin kann der Subcode SC auf dem Flash-Speicher 2 ganz oder teilweise verschlüsselt abgelegt sein. Auch für diese Verschlüsselung kann die ID der einzelnen Speicherbausteine oder des Microrechners bzw. ein Teil dieser ID in den Schlüssel integriert werden. Die Entschlüsselung der Daten in dem Sub-Code wird durch den Master-Code durchgeführt. Da dieser in einem lesegeschützten Bereich des Microrechners abgelegt ist, kann ein Auslesen des Programms und damit eine Vervielfältigung der Software verhindert werden.

Die Überwachung des Sub-Codes gegenüber Manipulation, die durch den μC im Master-Code sichergestellt wird, kann auch über andere Verfahren als die Verschlüsselung erfolgen. So können zusätzlich oder alternativ lineare/CRC-Checksummenbildung oder Hash-Wertbildung verwendet werden. Zur Erkennung einer vorgenommenen Manipulation der Daten und gegebenenfalls Teile des Subcodes werden z.B. über ausgewählte Bereiche lineare Checksummen gebildet und das Ergebnis verschlüsselt als Fingerprint in den Sub-Code eingebracht. Der Mastercode berechnet im Steuergerätebetrieb, beispielsweise bei einem Signal an Klemme 15, über den gleichen vordefinierten Bereich den Vergleichswert (z.B. lineare Checksumme) und prüft diesen gegen den entschlüsselten im Sub-Code verschlüsselt abgelegten Referenzwert. Die Art der Manipulationserkennung kann beliebig gewählt werden.

Nach der Erkennung einer Manipulation werden vom Master-Code Maßnahmen eingeleitet, die gegebenenfalls zum Steuergeräteausfall führen.

In Figur 3 ist eine weitere Ausführungsform des erfindungsgemäßen Steuergeräts gezeigt. Bei dieser Ausführungsform sind die Speicherbausteine 2 und 3 in den Microrechner μC integriert. Der μC weist hierbei einen embedded Flash-Speicher auf, wobei der E²PROM emuliert wird. Diese Ausgestaltung des Steuergeräts weist zwar den Vorteil auf, dass ein Austausch der Speicherbausteine zuverlässig verhindert werden kann, allerdings sind die Daten bei der Emulation des E²PROM nur blockweise überschreibbar.

Das Verfahren zum Schutz gegen Manipulation erfolgt bei diesem Steuergerät mit internem Speicher im wesentlichen wie das oben für Steuergeräte mit externen Speichern beschriebene. Auch hierbei können insbesondere die Daten des E²PROM verschlüsselt abgelegt werden und durch einen Schlüssel, der zumindest eine individuelle Kennung des Steuergeräts, wie die μC-

ID und/oder die Flash-ID umfasst, entschlüsselt werden. Ebenso können die in dem Subcode, der in dem Flash-Speicher des μC abgelegt ist, enthaltenen verschlüsselten Daten oder Fingerprints durch den Mastercode entschlüsselt werden. Auch hierbei wird vorzugsweise eine steuergeräteindividuelle Kennung in dem Schlüssel integriert.

Die Erfindung ist nicht auf die dargestellten Ausführungsformen beschränkt. So kann als Kennung der einzelnen Speicherbausteine beispielsweise das Herstellungsdatum des Steuergeräts in Betracht kommen. Hierdurch kann eine Manipulation während der Garantiezeit verhindert werden.

Das Steuergerät kann im Sinne dieser Erfindung beispielsweise ein Motorsteuergerät, ein Getriebesteuergerät oder auch ein Kombiinstrument darstellen.

Mit einem erfindungsgemäßen Verfahren und dem erfindungsgemäßen Steuergerät können gegenüber herkömmlichen Steuergeräten eine große Anzahl von Vorteilen erzielt werden.

Mit dem erfindungsgemäßen Steuergerät kann auf zuverlässige Weise ein Austausch einzelner oder mehrerer Bausteine verhindert werden, da durch einen solchen Austausch die Funktion des Steuergeräts verhindert werden kann. Das Auslesen eines für die Funktion der Steuerung zwingend erforderlichen Teils des Programms bzw. der Daten ist nicht möglich, wenn dieser Teil in dem lesegeschützten OTP-Bereich abgelegt ist. Damit kann eine Vervielfältigung der Software verhindert werden. Auch ist der Zugriff auf vertrauliche Daten über die Kontaktierung des Bausteins nicht möglich, wenn diese in dem lesegeschützten OTP-Bereich des μC abgelegt sind. Besonders sicher kann das Steuergerät vor Manipulationen geschützt werden, indem es nur in der Kombination von Master- und Sub-Code lauffähig ist. Eine Veränderung des im reprogrammierbaren, gegebenenfalls externen Speicher, z.B. Flash, abgelegten Sub-Codes führt ohne eine Anpassung des Mastercodes zu einem Steuergeräteausfall. Weiterhin können Daten, die beispielsweise auf einem E^2PROM abgelegt sind, steuergeräteindividuell verschlüsselt werden. Auch die Entschlüsselung solcher Daten kann von einer Kennung des Steuergeräts abhängig gemacht werden. Zusätzliche Sicherheit kann dadurch geschaffen werden, dass die Ver- und Entschlüsselung von dem Verbund der einzelnen Bausteine mit den dem μC bekannten ID's abhängig gemacht wird.

Zusammenfassend kann also festgestellt werden, dass durch die gewählte Verschlüsselung der Daten des E²PROMS die Manipulation von Steuergeräten, wie beispielsweise Chip-Tuning bei Motorsteuergeräten zuverlässig vermieden werden kann.

IP 4537
Th/Sc

Patentansprüche

1. Verfahren zum Schutz vor Manipulation eines Steuergeräts für mindestens eine Kfz-Komponente, wobei das Steuergerät (1) zumindest einen Microrechner (μC) und mindestens einen Speicherbaustein (2, 3) umfasst, wobei zumindest einer der Speicherbausteine (2, 3) einen reversiblen Festwertspeicher (3) darstellt, dadurch gekennzeichnet, dass in den reversiblen Festwertspeicher (3) Daten abgelegt werden, die durch ein Verschlüsselungsverfahren verschlüsselt worden sind, und der in dem Verschlüsselungsverfahren verwendete Schlüssel zumindest einen Teil mindestens einer ursprünglichen bausteinspezifischen Kennung (ID) mindestens eines der Bausteine (μC, 2, 3) des Steuergeräts umfasst.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Kennung eine Kennung des Microrechners (μC) darstellt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Kennung eine Kennung eines weiteren Speicherbausteins (3) darstellt.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Schlüssel in dem RAM des Microrechners (μC) abgelegt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass zur Erzeugung eines Schlüssels zum Verschlüsseln von Daten auf einem reversiblen Festwertspeicher (3) aus einem lesegeschützten OTP-Bereich (11) des Microrechners mindestens ein Teil einer Kennung (ID) mindestens eines der Bausteine (μC, 2, 3) des Steuergeräts (1) ausgelesen wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass bei jeder Inbetriebnahme des Steuergeräts (1) ein Schlüssel zum Entschlüsseln der in dem reversiblen Festspeichers (3) verschlüsselt abgelegten Daten neu erzeugt wird.

7. Steuergerät, in dem ein Verfahren nach einem der Ansprüche 1 bis 6 realisiert ist.

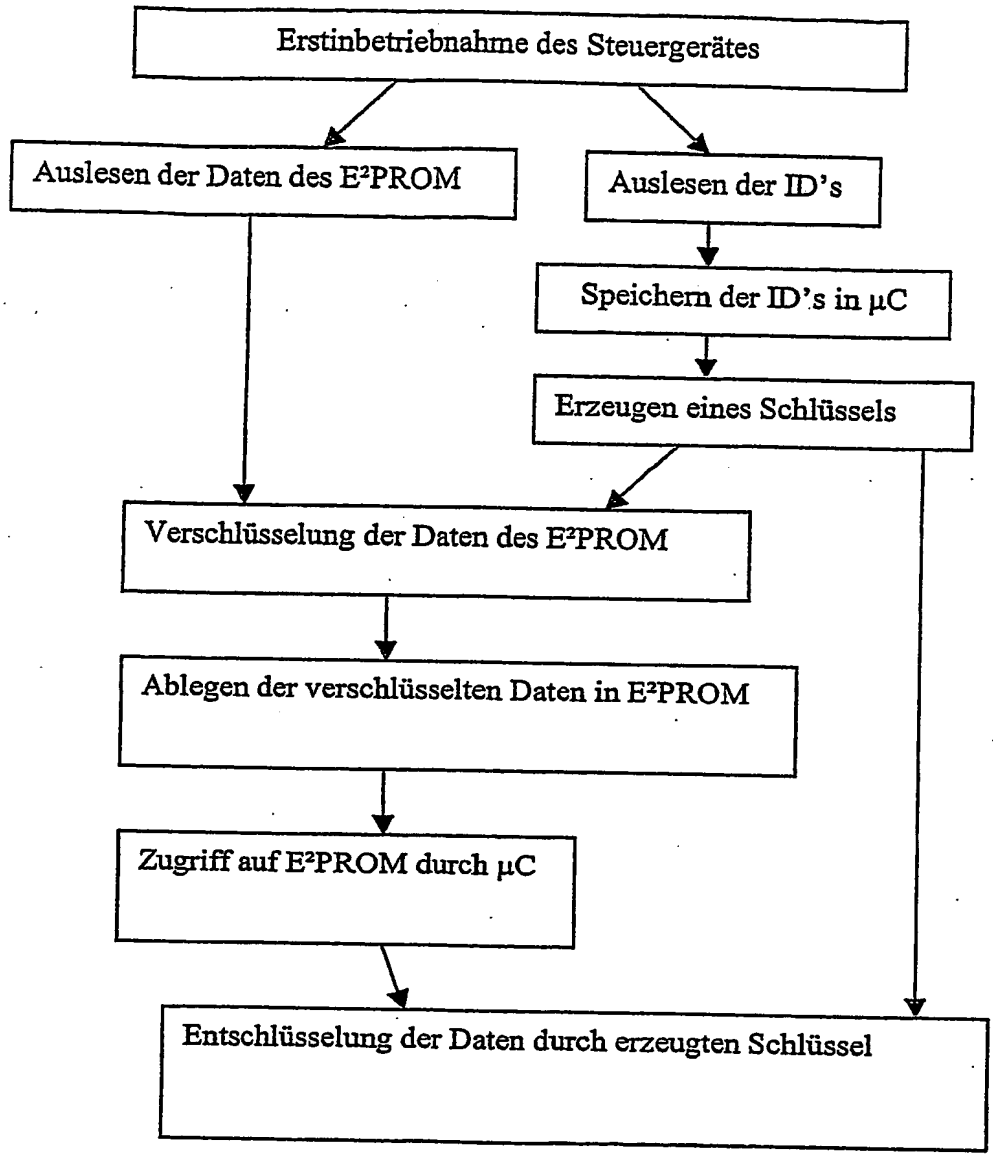


FIG. 1

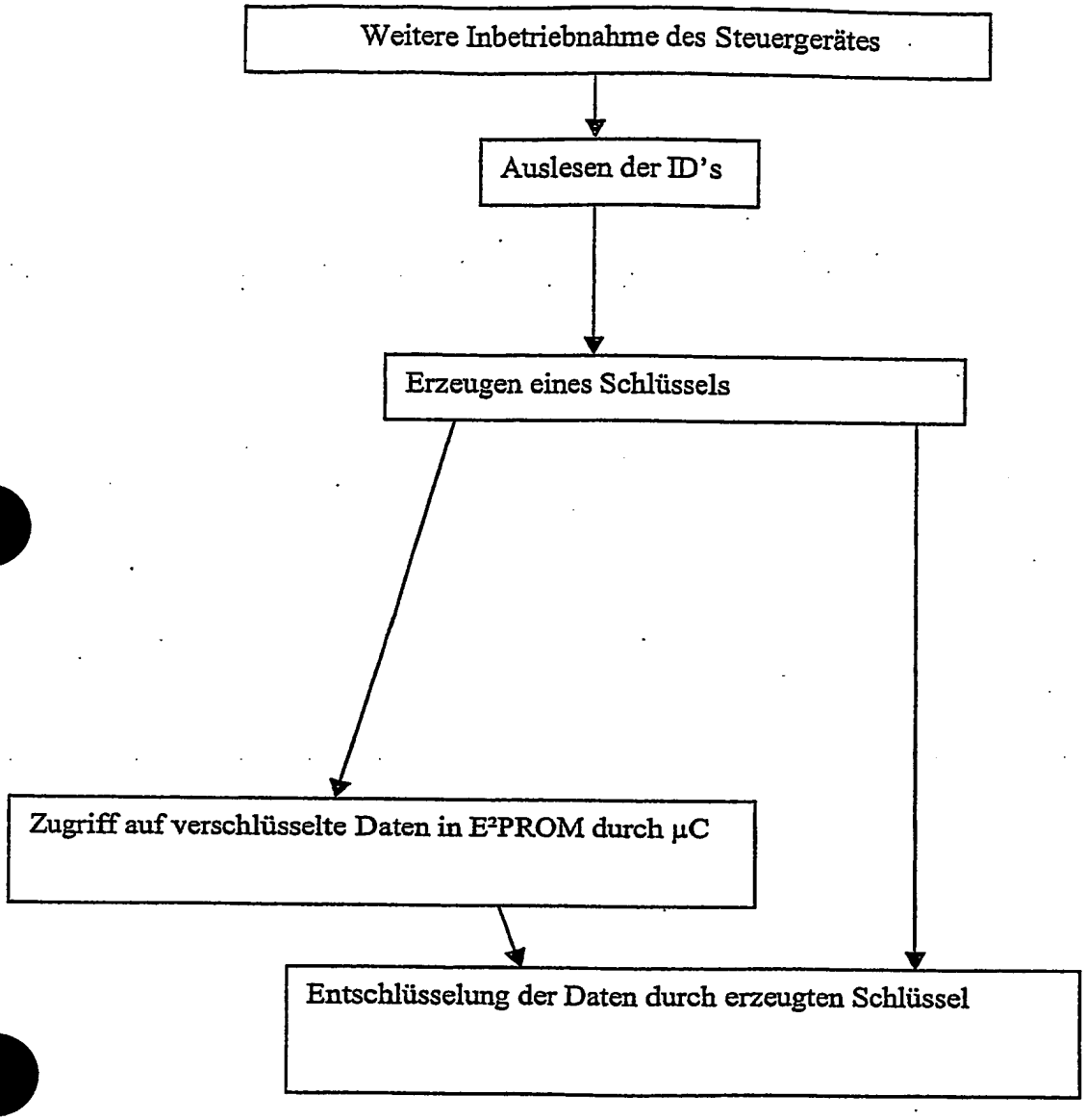


FIG. 1a

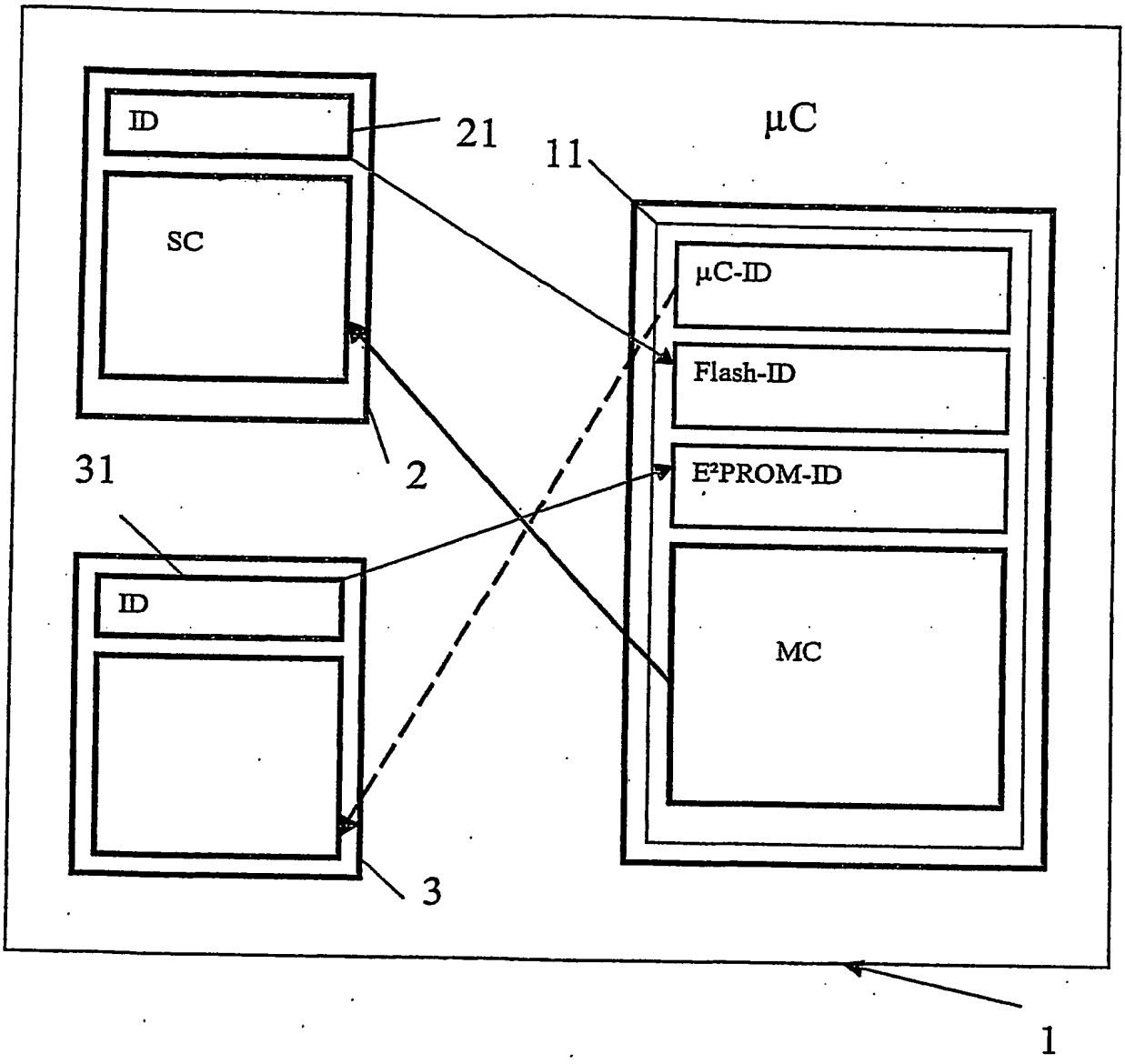


FIG. 2

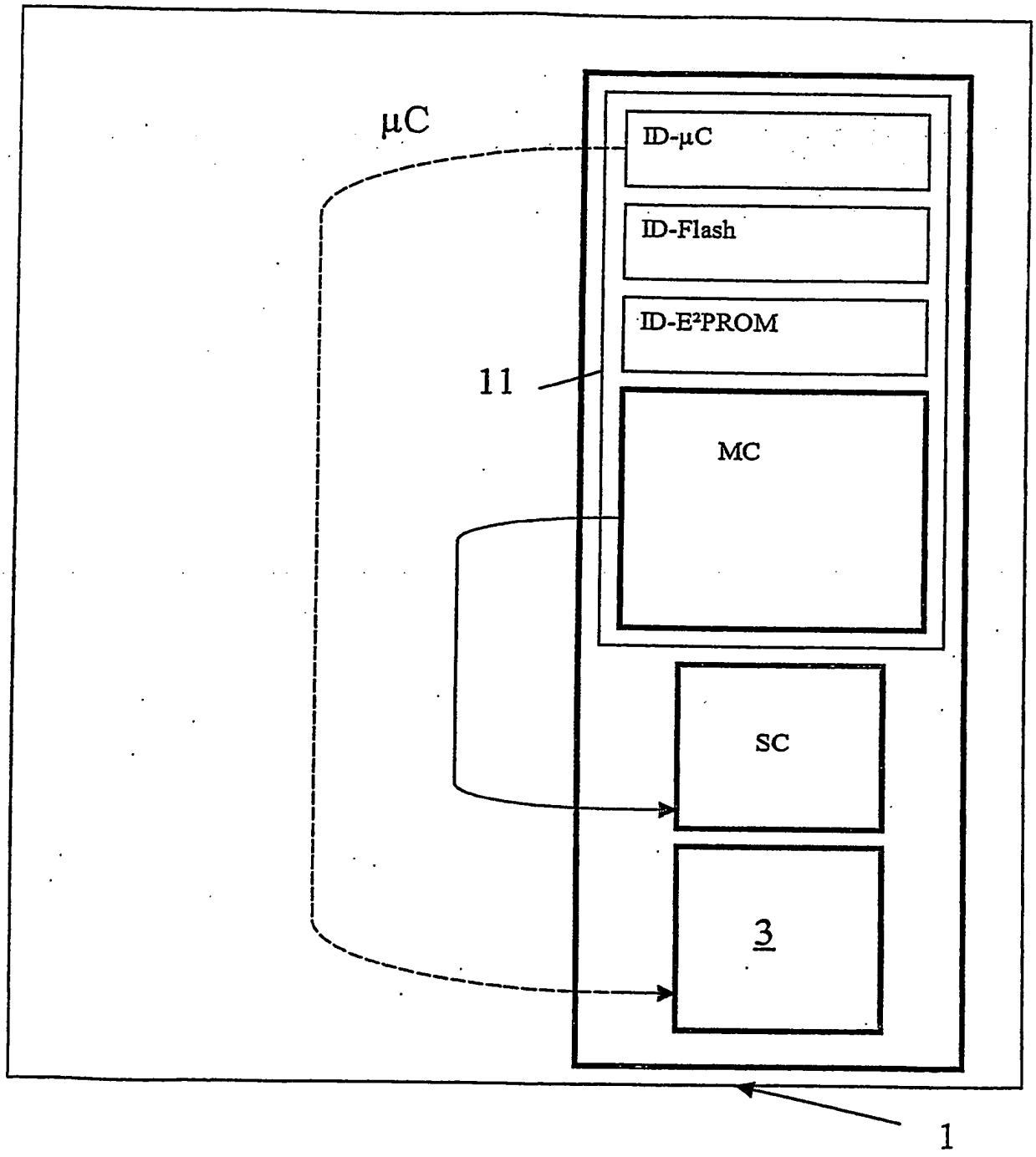


FIG. 3

IP 4537
Th/Sc

Zusammenfassung

Die Erfindung betrifft ein Verfahren zum Schutz vor Manipulation eines Steuergeräts für mindestens eine Kfz-Komponente, wobei das Steuergerät (1) zumindest einen Microrechner (μC) und mindestens einen Speicherbaustein (2, 3) umfasst, wobei zumindest einer der Speicherbausteine (2, 3) einen reversiblen Festwertspeicher (3) darstellt, dadurch gekennzeichnet, dass in den reversiblen Festwertspeicher (3) Daten abgelegt werden, die durch ein Verschlüsselungsverfahren verschlüsselt worden sind, und der in dem Verschlüsselungsverfahren verwendete Schlüssel zumindest einen Teil mindestens einer ursprünglichen bausteinspezifischen Kennung (ID) mindestens eines der Bausteine (μC, 2, 3) des Steuergeräts umfasst.

(mit Figur 2)

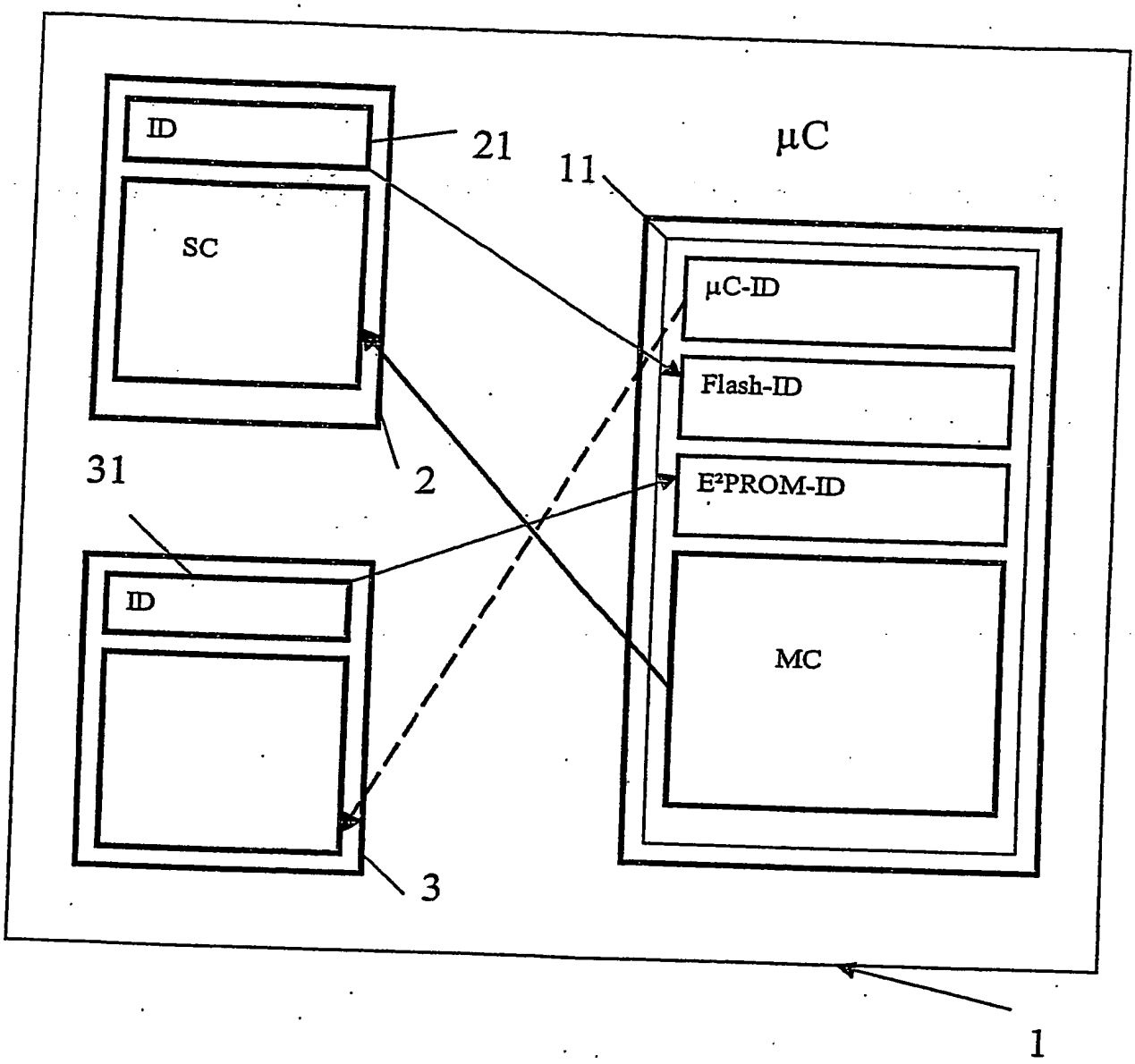


FIG. 2